

Attacking Encryption: Understanding risk and making intelligent choices

Unless you've been asleep for the last decade, you're aware that computer systems – enterprise and personal – are under attack from bad actors, ranging from script kiddies to state-sponsored teams. Encryption is one of the layers of defense keeping data from being stolen, disclosed, and monetized.

Yet we also hear about encryption weaknesses, in popular-press stories and more formal reports such as CVEs (“Common Vulnerabilities and Exposures”) maintained by the United States Department of Homeland Security (DHS).

What does it mean to “attack” encryption and how is it done? How do you decide what's realistic, and choose the right encryption approach for a given use case?

This session discusses types of encryption attacks at a non-crypto-geek level. It aims to help mere mortals gain a comfort level with the terminology, to help realistically appraise news stories about various crypto compromises, and to learn how to make good crypto choices.